

WHAT IS CLAIMED IS:

5           1. A system for securing an application for execution on a computer, the system comprising:

          a server computer;

          a network; and

          a client computer operably connected to the server computer via the network;

10           wherein the client computer requests the server computer to transmit an application to the client computer,

          wherein the client computer executes the application subsequent to receiving the application; and

15           wherein the client computer includes an interception module for intercepting a request from the application to output data to an output device, wherein the interception module ignores the request, and wherein the interception module returns a success message to the application.

20           2. A method of securing an application for execution on a computer, the method comprising:

          modifying a binary of the application such that a request to affect the visible properties of a window is intercepted by an interception module;

          ignoring the request; and

          returning a success message to the requestor.

25           3. A method of securing an application for execution on a computer, the method comprising:

          modifying a binary of the application such that a request from the application to output data to an output device is intercepted;

          ignoring the request; and

30           returning a success message to the requestor.

4. The method of Claim 3, additionally comprising inserting in an import table a reference to an interception module, wherein the reference is inserted in the import table such that the interception module is invoked in response to loading of the application, and wherein the interception module intercepts the request from the requestor.

5. A method of securing an application for execution on a computer, the method comprising:

modifying the binary of an application to invoke an interception module;  
intercepting a request from the application to create and display a window on an output device;  
setting a property of the window such that the window is not displayed on the output device; and  
creating the window.

6. The method of Claim 5, additionally comprising inserting in an import table a reference to an interception module, wherein the reference is inserted in the import table such that the interception module is invoked in response to loading of the application, and wherein the interception module intercepts the request from the requestor.

7. A method of securing an application for execution on a computer, the method comprising:

modifying the binary of an application to invoke an interception module;  
intercepting a request from an application to send a message from the application to a window;  
modifying the message such that the message does not affect any visible properties of the window; and  
transmitting the modified message to the window.

8. A method of securing an application for execution on a computer, the method comprising:

modifying the binary of an application to invoke an interception module;  
intercepting a request from an application to display a decision box;  
5 identifying a decision for the decision box; and  
transmitting the identified decision to the decision box.

9. The method of Claim 8, additionally comprising transmitting the decision to a management process for evaluation.

10. A system for securing an application for execution on a computer, the system comprising:

means for modifying the binary of an application to invoke an interception module;  
15 means for intercepting a request from the application to output data to an output device;  
means for ignoring the request; and  
means for returning a success message to the application.

11. The system of Claim 10, additionally comprising means for inserting in an import table a reference to an interception module, wherein the reference is inserted in the import table such that the interception module is invoked in response to loading of the application, and wherein the interception module intercepts the request from the requestor.

12. A system for securing an application for execution on a computer, the system comprising:

means modifying the binary of an application to invoke an interception module;  
means for intercepting a request from the application to create and display a  
30 window on an output device;  
means for creating the window; and

means for setting a property of the window such that the window is not displayed on the output device.

5 13. The system of Claim 12, additionally comprising means for inserting in an import table a reference to an interception module, wherein the reference is inserted in the import table such that the interception module is invoked in response to loading of the application, and wherein the interception module intercepts the request from the requestor.

10 14. A system for securing an application for execution on a computer, the system comprising:

a first module for modifying the binary of an application to invoke a

15 second module, wherein the second module intercepts a request from the application to output data to an output device, wherein the second module ignores the request, and wherein the second module returns a success message to the requestor.

20 15. A method of securing an application for execution on a computer, the method comprising:

modifying the binary of an application to invoke an interception module; and

25 intercepting at least one call that is made by the application such that the application cannot change the contents of a display that is connected to the computer.